IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.106100

SecureHealth: A Blockchain-Based Healthcare Application

Rounak Naik[1], Akshay Diwadkar[2], Hemang Bhagat Amonkar[3], Aniket Prabhu[4],

Mrs. Sherica Menezes[5]

Student, Computer Engineering Department, Goa College of Engineering, Ponda, India[1-4]

Professor, Computer Engineering Department, Goa College of Engineering, Ponda, India[5]

Abstract: This study uses blockchain technology to create a decentralized platform that is safe for storing and exchanging medical records. The technology guarantees tamper-proof and permanent records of patient data while giving patients control over their private health information. In order to improve healthcare services, the application will also offer some extra healthcare features like a doctor locator and area warnings. Medical records will be maintained on the decentralized storage network Arweave, while the application will be built on the Solana blockchain. This strategy will improve medical data security while ensuring quick access to medical records.

Keywords: Blockchain, Healthcare, Solana, Arweave

I. INTRODUCTION

Even though healthcare technology has advanced significantly, there are still some things that may be done better. The storing and retrieval of medical records, which are essential to a patient's care, is one such field. Medical records may take longer to access digitally and physically in emergency scenarios. Additionally, because medical information is private, it must be securely held to minimize hazards to consumers.

This initiative suggests putting medical records on a blockchain platform to overcome these problems, guaranteeing the security of the information and making it widely accessible. To further improve the healthcare system, we also intend to include features like Area Warnings and Doctor Locator. This blockchain-based platform will provide a tamper-proof and permanent record of patient data that can be accessed quickly and efficiently during emergencies thus improving patient care. By offering these features we aim to improve the healthcare sector and make it more efficient and secure for all.

II. LITERATURE SURVEY

A. *Blockchain*

To develop a tamper-proof and permanent record storage system for medical records, we look towards Blockchain, a distributed ledger shared among a computer network's nodes. Blockchain provides a characteristic of permanent storage of data which means that once data has been stored on it, it cannot be tampered with, damaged, or lost which is very important in the case of medical data. Though blockchain is most commonly used for cryptocurrency and financial applications, it can also be used in scenarios that require permanent and secure storage of data as well as in other scenarios.

To understand the concepts of Blockchain such as Proof of Work we referred to the Bitcoin whitepaper [1].

As mentioned above, Blockchain is a decentralized and distributed ledger shared among a computer network's nodes. It is basically a database that stores data in blocks that are connected to each other using cryptography. It is an ever-growing list of blocks that are stored in an ordered fashion. A block consists of the transaction data, the hash of the previous block, and the timestamp

One of the biggest features of blockchain is its immutability which can be used for making any data immutable. Hence, it has a big use case in areas that demand security and immutability of data. Since blockchain is a distributed ledger, it

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.106100

has its copies stored across many computers, hence altering a block or record is not possible without altering all subsequent blocks and the consensus of the network. This means that in order to alter a block, the same changes will have to be made on at least the majority number of copies of that block which are stored on other systems in order for the block to be accepted by the network. Though possible it's a very difficult and expensive task. This use case makes it well suited for storing medical data as medical data is very critical information and should never be tampered with or lost.

As explained in The Bitcoin Whitepaper [1], it uses the concept of a Timestamp Server. It operates by creating a hash of the items that need to be timestamped and then making that hash publicly available. This demonstrates that the data had to have been present at that moment in order to be part of the hash. A chain is formed by the timestamps, each of which hashes the one before it. The paper also introduces the concept of Proof of Work. The Proof of Work concept used in Bitcoin [1] involves finding a value that when hashed with a suitable hashing algorithm, the hash starts with a certain number of zero bits. Each block in the network has a nonce attached to it, and the proof of work is accomplished by increasing the nonce until a value is discovered that gives the block an appropriate hash. Once the hash has been calculated, changing the block is not possible without redoing the work and possibly redoing all the blocks which have been chained after it. The Bitcoin paper [1] also discusses various other concepts about the network which have been very crucial for us in understanding the working of blockchain.

The Solana whitepaper [4] explains the architecture of the Solana blockchain and also introduces the concept of Proof of History. According to the definition given in that work, it is a series of calculations that can be used to cryptographically confirm the passage of time between two events. It makes use of a cryptographically secure function that was created so that the output could not be predicted from the input and that it had to be fully performed in order to produce the outcome. The function is called repeatedly, with the previous output serving as the current input and the current output is regularly recorded. With each sequence segment checked on a distinct core, the output can then be recalculated and confirmed by external computers in parallel. Data can be timestamped into this sequence by appending it to the state of the function. A timestamp provided by the recording of the state, index, and data as they were added to the sequences ensures that the data was created before the next hash in the sequence.

As explained in the work, the proof of history works as follows, we use a cryptographic hash function whose output cannot be predicted without running the function and is collision-resistant. We start with a random value and compute its hash using the function. This hash is passed as the input during the next execution of the function and so on. If at any iteration of the algorithm, we need to append data then we can simply combine the data with the hash and generate the next hash. This concept makes it impossible to predict the hash value at iteration n without actually running the function with starting value for n-1 times. Thus, it can be inferred that real-time has passed between iterations 0 to n.

B. *Existing Systems*

The MedRec research paper proposes a novel, decentralized record management system to handle EMRs, using blockchain technology [2]. Their solution provides patients with an unchangeable log and simple access to their health data across providers and treatment locations. MedRec employs smart contracts on the Ethereum blockchain to record patient-provider connections that link a medical record with viewing permissions and data retrieval instructions.

In the Blockchain-Based Data Preservation System for Medical Data research paper [3], they have proposed a novel blockchain-based data preservation system for medical data. By using their system, users can keep medical data indefinitely and have the ability to verify the data's authenticity to look for tampering. They have developed the system using the Ethereum blockchain.

We expand on these concepts and develop a blockchain-based platform that provides easy storage, access, and sharing of medical data among different medical service providers with the patient's authorization. The proposed system has been developed using the Solana [4] and Arweave [5] blockchains. The low transaction cost of Solana and the low storage cost of Arweave makes the proposed system affordable.

III. DESIGN AND IMPLEMENTATION

A. *Overview*

While our main aim through SecureHealth is to provide common, secure storage of medical data such that it is accessible

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.106100

across various healthcare providers, we have also focused on some other aspects of healthcare that we felt needed addressing which could improve the health services provided to the public. These features are Area Warnings, Doctor Locator, and Routine Setter and Tracker. This section presents an overview of the various features implemented by us in the application and their basic working.

B. *Storage of Medical Data on Blockchain*

Throughout the course of one's life, a person produces a large amount of medical data, be it just normal checkups due to illness or medical reports. Handling such large amounts of data physically is a troublesome issue and there may also be a loss of critical medical information.

Before starting a patient's treatment, clinicians must have a thorough awareness of their medical history, including any prior allergies or underlying problems. This information is crucial for selecting the best course of treatment.

In emergency cases, it can become really difficult to gather all the physically stored medical reports of the concerned patient and incomplete information related to a patient's medical history can lead to inefficient treatment. In some cases, it can also lead to further worsening of the patient's health condition and sometimes even death.

Medical data can still be altered or erased even if it is kept online on a cloud or other similar storage systems, which can again result in the problems listed above.

The proposed application uses a blockchain-based storage model for all types of medical data, be it normal checkups or medical reports. We have two separate methods for storing medical reports(files) and for storing medical checkup data on the blockchain. The Solana blockchain has been used in both methods as the final point where the data gets stored. We have written a different Solana program for each of the methods.

Since Solana does not allow the storage of files directly on it, the first method uses the Arweave blockchain in addition to Solana for the storage of files. Arweave [5] allows us to store data permanently on it which accurately suits our purpose of storing medical data permanently.

To uphold patient privacy and security when storing medical data on the blockchain, it is essential to refrain from uploading personal details, including patients' names. Instead, in our proposed application patients are identified using unique Patient IDs. By associating medical reports and checkup data with these identifiers, the confidentiality of individuals is preserved. This approach ensures secure storage and retrieval of medical data from the blockchain while safeguarding the privacy of patients.

For storing a medical report i.e., a file, we first upload it to Arweave and retrieve its file ID, a unique identifier generated by Arweave for the file using which it can be accessed. The file ID is encrypted for security purposes and then along with the Patient ID of the patient, Doctor ID of the doctor who has examined the patient, and the Timestamp of uploading is passed to the Solana Program which uploads these details onto a newly created Solana Account while also taking some additional security measures. The Solana Account address on which these details are stored along with the generated transaction ID for this particular transaction is stored on our database to allow easy retrieval of data at any later point in time. Algorithm in Fig. 1 depicts this process of storing a medical report on the blockchain.

Algorithm 1 Algorithm for Uploading Medical Reports(Files)

Input: Patient_ID, Doctor_ID, file
1: file_id ← *upload file to arweave*
2: Encrypt the file ID using an encryption algorithm
3: timestamp ← *retrieve the current timestamp*
4: account_address ← *generate a new solana account address*
5: Initialize the account using the Solana Program
6: transaction_id ← *Pass the Patient_ID, Doctor_ID, encrypted file_id and timestamp to the Solana Program which uploads the data to the account*
7: Return the account_address and transaction_id

Fig. 1 Algorithm for Uploading Medical Reports (Files)

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.106100

The Anchor implementation of the structure of the Solana Account used to store medical reports has been shown below in Fig. 2.

```
#[account]
pub struct BaseAccount {
    pub pid: String,
    pub did: String,
    pub title: String,
    pub fid: String,
    pub timestamp: String,
    pub access_count: u64,
}
```

Fig. 2 Solana Account Structure to store Medical Reports

Since checkup-related data of a patient is mostly textual data entered by the doctor such as symptoms, diagnosis, prescription, and so on, it can be directly stored on Solana, and using Arweave isn't necessary. Since in the case of checkup-related data, there are additional fields for storing subject (title of the checkup), description (includes symptoms, diagnosis, etc.), and prescription, we have used a different Solana account structure for storing checkup data. The Anchor implementation of the structure of the Solana Account used for storing checkup data is shown below in Fig. 3.

```
#[account]
pub struct CheckupAccount {
pub pid: String,
pub did: String,
pub subject: String,
pub description: String,
pub prescription: String,
pub timestamp: String,
pub access_count: u64,
}
```

Fig. 3 Solana Account Structure to store Checkup Data

Before uploading the checkup data on the blockchain, the subject, description, and prescription are encrypted for security purposes. They are then passed to the Solana program along with the Patient ID of the patient, Doctor ID of the doctor who has diagnosed the patient, and the Timestamp of uploading, which then uploads these details to a newly created Solana Account. Just like in the case of medical reports, the Solana account address and transaction ID are stored on our database for easy retrieval of this data from the blockchain at any later point in time. Algorithm in Fig. 4 depicts this process of uploading checkup data to the Solana blockchain

Algorithm 2 Algorithm for Uploading Medical Checkup Data

Input: Patient_ID, Doctor_ID, Subject , Description , Prescription

1: Encrypt the Subject, Description, and Prescription using an encryption algorithm

3: timestamp ← *retrieve the current timestamp*

4: account_address ← *generate a new solana account address*

5: Initialize the account using the Solana Program

6: transaction_id ← *Pass the Patient_ID, Doctor_ID, timestamp, and encrypted Subject, Description, and Prescription to the Solana Program which uploads the data to the account*

7: Return the account_address and transaction_id

Fig. 4 Algorithm for Uploading Medical Checkup Data to Blockchain

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.106100

As mentioned before, we have implemented two different Solana Programs for uploading medical reports and uploading medical checkup data. Both programs have been successfully deployed on the Solana Devnet. Since Solana Accounts are mutable, we have also implemented some additional security features to prevent tampering with the uploaded medical data. However, details regarding these specific security measures have not been disclosed in this paper to maintain confidentiality and protect the system against potential vulnerabilities or exploits. The focus of this paper is to provide an overview of the implementation and functionality of the Solana Programs for medical data storage while keeping sensitive security measures undisclosed.

Medical Data including reports as well as checkups can only be uploaded by the Hospital or the Clinic. Once uploaded to the blockchain, the patient will have complete control over their medical data and no one else can access it without the patient's permission. Through the process of OTP verification, the patient must have granted the hospital or clinic access to their medical data in order for its doctors to be able to view it. Our system also allows patients to revoke permission for accessing their medical data at any time.

Though the process of storing medical reports slightly differs from the process of storing checkup data, the process of retrieval is mostly the same for both.

Upon receiving the Account Address and Transaction ID of a specific medical report or checkup, a verification process is initiated to ensure the integrity of the data stored in the Solana Account.

Both the transaction IDs—one received as input and one from the blockchain—are compared to ensure that the data hasn't been altered because the transaction of uploading the data to the account was recorded on the blockchain.

If the transaction IDs match and the data is not tampered then fields that were encrypted earlier are decrypted and all the details stored on the account are returned to be displayed to the requesting doctor or the patient to whom the data belongs. Algorithm in Fig. 5 depicts this process of retrieving the stored medical data from the blockchain.

Algorithm 3 Algorithm for Retrieving Medical Records/Checkups

Input: Account_Address, Transaction_ID
last_transaction ← *Retrieve the last transaction_id of the account recorded on the blockchain*
if last_transaction = Transaction_ID **then**
  Retrieve the data stored in the account using the Account_Address
  Decrypt the encrypted fields from the retrieved data
  Return the data stored in the Account
else
  Report that the data was tampered

Fig. 5 Algorithm for Retrieving Medical Records/Checkups

C. *Area Warnings*

During the Covid-19 outbreak, it had become challenging to move out of our houses as there was a high possibility of getting infected with the Covid virus. Along similar lines, there are possibilities of getting infected with many other existing communicable diseases like the Common Cold, Malaria, Tuberculosis, etc if we visit any highly infected areas or come in contact with an infected person.

So, to make people more informed about rising cases of any particular communicable diseases in an area, the Area Warning module has been implemented in this application where the hospitals or clinics can mark the patient who has been diagnosed with any communicable/infectious diseases. The addresses or locations of infected patients will then be plotted on a map on our user-end application. This will help other users to avoid moving into infected areas and thus will prevent the mass spread of infection.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.106100

It is important to note that only the locations of the infected patients will be shown on the map without disclosing any other details about them thus upholding their privacy. The user can see the cases of any particular disease at any location on the map which will help them to take precautions and also plan their travels properly.

D. *Doctor Locator*

In times of emergencies, people generally try to seek specialist doctors for treatments. If the doctor isn't available in the hospital, then it may lead to unnecessary delays and even the patient's life could be at risk.

To avoid this, a Doctor Locator module has been introduced in our application, in which the users can search for any doctors registered in our application by their name, by hospital name, or by doctor's specializations. The search result will show the basic details of the doctor and most importantly it will display whether the doctor is available currently at the registered hospital they work in or not.

Doctor's availability status can be updated by the hospital as well as doctors based on their schedule and preferences. This flexibility allows doctors to turn on and off their availability status at their convenience. With this feature, patient or their guardians will be in a better position to make a choice of which hospital to visit for better and fast treatment.

E. *Routine Setter and Tracker*

When patients are prescribed medication for a certain period, it becomes a hassle to keep track of the days the medicine was taken and the days it wasn't. Self-reporting of the medicine use to the doctor also becomes a game of perfect memory. To resolve these issues the Routine Setter and Tracker feature has been introduced in our proposed application, where patients can set their medication routines, medically prescribed physical activity, and appointment reminders for certain specified time periods. All this progress can be tracked easily giving a clear status of the treatment history. When the user sets a reminder for a specified time and for specified days, they get notifications for that particular reminder accordingly. If the user uses a smart-watch or a smart band, upon giving notification permission to our application in their smart-wearable application, one can get notified about the reminders even on their wearables.

One of the concerns that came up during discussions with doctors was the issue regarding patients' adherence to treatment routines. Doctors reported that even though a well-planned routine was provided to the patients, the patients were not adhering to that prescribed routine till the time of its completion, hence not obtaining the required results. To resolve this issue, gamification and incentivization have been introduced in the Routine Setter and Tracker. This has been achieved using Tree Animation. The tree grows as per the percentage of completion for a particular routine. Upon a 100 percent completion of let's say ten routines, the user will receive a reward that enables the user to have one free report upload or other similar rewards.

IV. CONCLUSION AND FUTURE SCOPE

In this paper, we have presented a blockchain-based healthcare application with our main goal being to create a common, decentralized, and secure storage for all medical records of a patient. The proposed system allows easy storage and sharing of medical records between healthcare service providers while also giving a patient complete control over their medical data as none of the records are associated with a hospital or stored on their own database. Using Arweave and Solana, we have ensured tamper-proof and permanent storage of medical records.

Compared to traditional physical storage of medical records, our system provides a more secure and easy way of storing them which helps in preventing loss as well as tampering of critical medical data. Since all the data is stored in one place, it also makes it easier to retrieve the medical history of the patient quickly in emergency cases so that doctors can start treatment without much delay.

In the case of emergencies, the Doctor Locator feature allows users to find specialists and the best possible doctors who are currently available so that not much time is wasted. The Area Warnings feature of our system helps users in making informed decisions and take precautions about any rising cases in their area or while traveling to a certain location. The Routine Setter and Tracker is an essential module that can be very helpful for people in the current busy world as we tend to forget things. Gamification and incentivization also provide additional motivation for users to complete their routines.

DOI: 10.17148/IARJSET.2023.106100

In the near future, we intend to make our application ABHA (Ayushman Bharat Health Account) compliant and contribute to the Indian Government's initiative Ayushman Bharat Digital Mission (ABDM). This includes providing our application to the local healthcare bodies and helping them connect with ABHA.

In order to improve the security of the uploaded medical reports, encryption of the files or using private folders on Arweave for storage can also be explored.

For the purpose of verification and identification, biometric systems such as face and fingerprint recognition can also be implemented in the future which will help to access the concerned patient's medical data in emergency cases.

We also intend to make it a one-stop destination for all health-related facilities by adding necessary features like online appointments, virtual consultations, Pharmacies, and Pathology labs integration.

ACKNOWLEDGMENT

We thank the principal, head of the department, and faculty at the Computer Engineering Department and the Goa College of Engineering for giving us this opportunity and guiding us with our work. We are also thankful to all the authors of the research papers that we have referred to in our work.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Bitcoin, 2006.
[2] “MedRec: Using Blockchain for Medical Data Access and Permission Management,” IEEE Conference Publication | IEEE Xplore, Aug. 01, 2016.
[3] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, “Blockchain-Based Data Preservation System for Medical Data,” Journal of Medical Systems, vol. 42, no. 8, Jun. 2018, doi: 10.1007/s10916-018-0997-3.
[4] A. Yakovenko, “Solana: A new architecture for a high performance blockchain v0.8.13,” Solana, Nov. 2020. https://solana.com/solana-whitepaper.pdf
[5] “Arweave AR whitepapers - whitepaper.io.”
[6] “An Innovative IPFS-Based Storage Model for Blockchain,” IEEE Conference Publication | IEEE Xplore, Dec. 01, 2018.
[7] “A Comprehensive survey on Blockchain: Working, security analysis, privacy threats and potential applications,” IEEE Conference Publication | IEEE Xplore, Jul. 01, 2019.
[8] Nofer, M., Gomber, P., Hinz, O. et al. Blockchain. Bus Inf Syst Eng 59, 183–187 (2017). https://doi.org/10.1007/s12599-017-0467-3